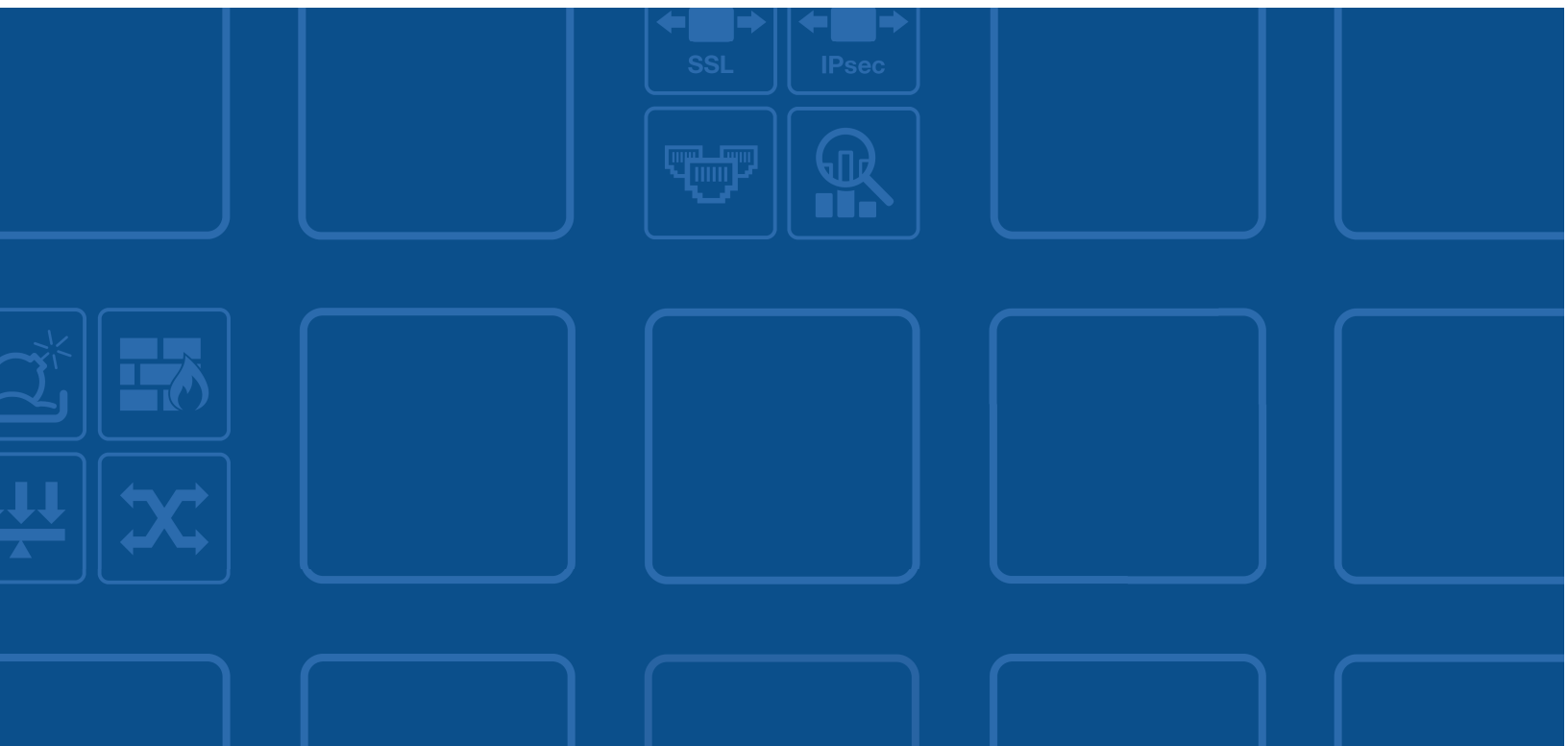
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.4.5



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 22, 2017

FortiOS 5.4.5 Release Notes

01-545-424040-20171222

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-06-08	Initial release of FortiOS 5.4.5.
2017-06-09	Added 403937 to *Resolved Issues*. Updated *Upgrade Information > Upgrading to FortiOS 5.6.0*. Updated 435124 in *Known Issues*.
2017-06-13	Removed 416678 from *Known Issues*. Added 398052 to *Resolved Issues*. Added FGT-140 and FGT-140-POE to *Introduction > Supported models > Special branch supported models*.
2017-06-15	Added 399711, 421739, and 423452 to *Resolved Issues*.
2017-06-26	Added 389863 to *Resolved Issues*.
2017-06-30	Removed 374501 from *Resolved Issues* since that was resolved in 5.4.4. In *Product Integration and Support* section, updated FortiClient support to 5.4.1 and later.
2017-07-12	Added 424215 to *Known Issues*.
2017-07-21	Added 439923 to *Known Issues*.
2017-07-31	Added 398424 to *Resolved Issues*.
2017-08-02	Added 409913 to *Resolved Issues*.
2017-08-08	Added Windows 2016 Server Edition and Windows 2016 Datacenter to *Product Integration and Support*. Added 408239 to *Resolved Issues*.
2017-08-21	Added 435283 to *Known Issues*.
2017-08-25	Added *DLP, AV* section to *Special Notices*.
2017-09-05	Added 408321 to *Known Issues*.
2017-09-18	Added 413699 to *Known Issues*.

Date	Change Description
2017-10-16	Added 410521 to *Resolved Issues*.
2017-11-10	Added 273973 to *Known Issues*.
2017-12-22	Added FG-7000E to *Introduction* > *Supported models* > *Special branch supported models*.

Introduction

This document provides the following information for FortiOS 5.4.5 build 1138:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.4.5 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30D-POE, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30D-POE, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE
FortiGate Rugged	FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN FortiOS 5.4.5 supports the additional CPU cores through a license update on the following VM models: • VMware 16, 32, unlimited • KVM 16 • Hyper-V 16, 32, unlimited
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.4.5 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS 5.4.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1138.

FGR-30D	is released on build 7662.
FGR-35D	is released on build 7662.
FGR-30D-A	is released on build 7662.
FG-30E-MI	is released on build 6229.
FG-30E-MN	is released on build 6229.
FWF-30E-MI	is released on build 6229.
FWF-30E-MN	is released on build 6229.
FWF-50E-2R	is released on build 7657.
FG-52E	is released on build 6226.
FG-60E	is released on build 6225.
FWF-60E	is released on build 6225.
FG-61E	is released on build 6225.
FWF-61E	is released on build 6225.
FG-80E	is released on build 6225.
FG-80E-POE	is released on build 6225.
FG-81E	is released on build 6225.
FG-81E-POE	is released on build 6225.
FG-90E	is released on build 6230.
FG-90E-POE	is released on build 6230.
FG-91E	is released on build 6230.
FWF-92D	is released on build 7660.
FG-100E	is released on build 6225.

FG-100EF	is released on build 6225.
FG-101E	is released on build 6225.
FG-140E	is released on build 6257.
FG-140E-POE	is released on build 6257.
FG-200E	is released on build 6228.
FG-201E	is released on build 6228.
FG-2000E	is released on build 6227.
FG-2500E	is released on build 6227.
FG-7000E	is released on build 6481.

What's new in FortiOS 5.4.5

For a detailed list of new features and enhancements that have been made in FortiOS 5.4.5, see the *What's New for FortiOS* 5.4.5 document available in the Fortinet Document Library.

Special Notices

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

Default log setting change

For FG-5000 blades, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

FortiAnalyzer Support

In version 5.4, encrypting logs between FortiGate and FortiAnalyzer is handled via SSL encryption. The IPsec option is no longer available and users should reconfigure in GUI or CLI to select the SSL encryption option as needed.

Removed SSL/HTTPS/SMTPS/IMAPS/POP3S

SSL/HTTPS/SMTPS/IMAPS/POP3S options were removed from server-load-balance on low end models below FG-100D except FG-80C and FG-80CM.

FortiGate and FortiWiFi-92D Hardware Limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form
- IPv6 packets being dropped
- FortiSwitch devices failing to be discovered
- Spanning tree loops may result depending on the network topology

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config system global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed
- BPDUs are dropped and therefore no STP loop results
- PPPoE packets are dropped
- IPv6 packets are dropped
- FortiSwitch devices are not discovered
- HA may fail to form depending the network topology

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FG-3700DX

CAPWAP Tunnel over the GRE tunnel (CAPWAP + TP2 card) is not supported.

FortiGate units managed by FortiManager 5.0 or 5.2

Any FortiGate unit managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

FortiClient Support

Only FortiClient 5.4.1 and later is supported with FortiOS 5.4.1 and later. Upgrade managed FortiClients to 5.4.1 or later before upgrading FortiGate to 5.4.1 or later.

Consider the FortiClient license before upgrading. Full featured FortiClient 5.2 and 5.4 licenses will carry over into FortiOS 5.4.1 and later. Depending on your organization's needs, you might need to purchase a FortiClient EMS license for endpoint provisioning. Contact your sales representative for guidance on the appropriate licensing for your organization.

The perpetual FortiClient 5.0 license (including the 5.2 limited feature upgrade) will not carry over into FortiOS 5.4.1 and later. You need to purchase a new license for either FortiClient EMS or FortiGate. A license is compatible with 5.4.1 and later if the SKU begins with FC-10-C010.

FortiClient (Mac OS X) SSL VPN Requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.5, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

FortiClient Profile Changes

With introduction of the Cooperative Security Fabric in FortiOS, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

In the FortiClient profile on FortiGate, when you set the *Non-Compliance Action* setting to *Auto-Update*, the FortiClient profile supports limited provisioning for FortiClient features related to compliance, such as AntiVirus, Web Filter, Vulnerability Scan, and Application Firewall. When you set the *Non-Compliance Action* setting to *Block* or *Warn*, you can also use FortiClient EMS to provision endpoints, if they require additional other features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

When you upgrade to FortiOS 5.4.1 and later, the FortiClient provisioning capability will no longer be available in FortiClient profiles on FortiGate. FortiGate will be used for endpoint compliance and Cooperative Security Fabric integration, and FortiClient Enterprise Management Server (EMS) should be used for creating custom FortiClient installers as well as deploying and provisioning FortiClient on endpoints. For more information on licensing of EMS, contact your sales representative.

FortiPresence

FortiPresence users must change the FortiGate web administration TLS version in order to allow the connections on all versions of TLS. Use the following CLI command.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

Log Disk Usage

Users are able to toggle disk usage between Logging and WAN Optimization for single disk FortiGates.

To view a list of supported FortiGate models, refer to the FortiOS 5.4.0 Feature Platform Matrix.

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

FG-30E-3G4G and FWF-30E-3G4G MODEM Firmware Upgrade

The 3G4G MODEM firmware on the FG-30E-3G4G and FWF-30E-3G4G models may require updating. Upgrade instructions and the MODEM firmware have been uploaded to the Fortinet Customer Service & Support site. Log in and go to *Download* > *Firmware*. In the *Select Product* list, select *FortiGate*, and click the *Download* tab. The upgrade instructions are in the following directory:

.../FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

DLP, AV

In 5.2, Block page was sent to client with HTTP status code `200` by default. In 5.4 and later, Block page is sent to client with a clearer HTTP status code of `403 Forbidden`.

Upgrade Information

Upgrading to FortiOS 5.4.5

FortiOS version 5.4.5 officially supports upgrading from version 5.4.3 and later and 5.2.9 and later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is a separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.4 Supported Upgrade Paths.

Upgrading to FortiOS 5.6.0

If you have configured IPsec in version 5.4.5, after upgrading to 5.6.0, you must reconfigure all IPsec phase1 `psksecret` settings before you can establish an IPsec tunnel.

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 and later greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1 and later
- FortiClient EMS 1.0.1 and later
- FortiAP 5.4.1 and later
- FortiSwitch 3.4.2 and later

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
- *FortiOS 5.4.x Upgrade Guide for Managed FortiSwitch Devices*

  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

FortiGate-VM 5.4 for VMware ESXi

Upon upgrading to FortiOS 5.4.5, FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

When downgrading from 5.4 to 5.2, users will need to reformat the log disk.

Amazon AWS Enhanced Networking Compatibility Issue

Due to this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.4.1 or later image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

Downgrading to older versions from 5.4.1 or later running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.4.5 support

The following table lists 5.4.5 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Microsoft Internet Explorer 11 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 40 • Microsoft Internet Explorer 11 • Mozilla Firefox version 53 • Apple Safari version 10 (For Mac OS X) • Google Chrome version 58 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	For the latest information, see the FortiManager and FortiOS Compatibility. You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	For the latest information, see the FortiAnalyzer and FortiOS Compatibility. You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.4.1 and later If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading the FortiGate.
FortiClient iOS	• 5.4.1 and later
FortiClient Android and FortiClient VPN Android	• 5.4.0 and later

FortiAP	• 5.4.1 and later • 5.2.5 and later Before upgrading FortiAP units, verify that you are running the current recommended FortiAP version. To do this in the GUI, go to the *WiFi Controller > Managed Access Points > Managed FortiAP*. If your FortiAP is not running the recommended version, the *OS Version* column displays the message: *A recommended update is available*.
FortiAP-S	• 5.4.1 and later
FortiSwitch OS (FortiLink support)	• 3.5.0 and later
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 and later • 1.4.0 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0256 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Server Edition
	  • Windows Server 2016 Datacenter
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6.0 and later. Some FortiGate models may be supported on specific FortiExplorer versions.

FortiExplorer iOS	• 1.0.6 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 3.0.0 • 2.0.2 and later
AV Engine	• 5.247
IPS Engine	• 3.311
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

FortiGate-VM v5.4 for VMware ESXi (all models), no longer supports the VMXNET2 vNIC driver.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2333. Download from the Fortinet Developer Network https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 53 Google Chrome version 58
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 53
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 53 Google Chrome version 58
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔

Product	Antivirus	Firewall
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011	✔	✔
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 5.4.5. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
392200	Encrypted archive log is generated even though the function archive-log in antivirus profile is unset.

DLP

Bug ID	Description
379911	DLP filter order is not applied to encrypted files.

Firewall

Bug ID	Description
304276	Policy real time view shows incorrect statistic in session offload to np6.
378482	TCP/UDP traffic fais when NAT/UTM is enabled on FGT-VM in KVM.
395241	After IPS is enabled on LB-VIP policy, this message displays: `ipsapp session open failed: all providers busy`.
402158	Some policy settings are not installed in complex sessions.
416111	FQDN address is unresolved in a VDOM although the URL is resolved with IP.

GUI

Bug ID	Description
283682	Cannot delete FSSO-polling AD group from LDAP list tree window in FSSO-user GUI.
356998	`urlfilter` list re-order on GUI does not work.
371149	30D GUI should support FortiSwitch controller feature when CLI supports it.
372898	User group name should escape XSS script at *User Groups* page.

Bug ID	Description
374166	Using Edge cannot select the firewall address when configuring a static route.
374350	Field *pre-shared key* may be unavailable when editing the IPsec dialup tunnel created through the VPN wizard.
378428	FortiGate logs a connection of category *deny* (red sign) even though traffic is allowed through policy.
379331	DHCP *Monitor* page does not fully display the *page selector* pane.
384532	Cannot set IPsec `vpn xauth` user group *inherit from policy* in GUI when setting `xauthtype` auto server.
385482	Webui loads indefinitely when accessing a *none* access webpage from custom admin profile.
386285	GUI Wizard fails to create FortiClient Dialup IPsec VPN if HA is enabled.
386849	When editing IPsec tunnel, *Accessible Networks* field cannot load if there is nested address group.
387640	`Duplicate entry found` when auto generate guest user.
388454	GUI failures when FSSO group contains an apostrophe.
394067	Improve displaying the warning: *File System Check Recommended*.
395711	`pyfcgid` takes 100% of CPU when managed switch page displayed.
396430	CSRF token is disclosed in several URLs.
401247	Cannot nest service group within another service group through GUI.
409104	Fix virtual-wire wildcard VLANs not handling u-turn traffic properly.
421918	HTTPSD debug improvement.

HA

Bug ID	Description
373200	Quick failover occurs when enabling `portmonitor`.
382798	Master unit delay in sending heartbeat packet.
386434	HA configuration and VLAN interface disappear from config after reboot.

Bug ID	Description
396938	Reboot of FGT HA cluster member with redundant HA management interface deletes HA configuration.
397171	FIB of VDOMs in vcluster2 is not synced to the slave.
404736	SCTP synchronized sessions in HA cluster, when one reboots the master, the traffic is interrupted.
404874	Some commands for HA in `diag debug report` and `exec tac report` need to be updated.
408167	Heartbeat packets broadcast out of ports not configured as HB ports, even though the HB ports are directly connected.

IPsec VPN

Bug ID	Description
356330	Cross NP6-Chip IPsec traffic does not work in SLBC environment.
374326	*Accept type: Any peer ID* may be unavailable when creating a IPsec dialup tunnel with a pre-shared key and `ikev1` in main mode.
386802	Unable to establish phase 2 when using address group/group object as quick mode selectors.
392097	3DES encryption susceptible to Sweet32 attack.
395044	OSPF over IPsec IKEv2 with dialup tunnel does not work as for IKEv1.
397386	Slave worker blades attempt to establish site to site IPsec VPN tunnel.
409050	`unregister_netdevice` messages appears on console when CAPWAP message is transmitted over IPsec tunnel.
411682	ADVPN failover does not update *rtcache* entry.
412987	IPsec VPN certificate not validated against PKI user's CN and Subject.
410521	ADVPN IKE intermittently stops matching requests for an existing SPI.

Logging & Report

Bug ID	Description
377255	Can't read UTM details on log panel when set location to FortiAnalyzer.

Bug ID	Description
377733	*Results/Deny All* filter does not return all required/expected data.
386742	Missing deny traffic log when user traffic is blocked by NAC quarantine.
397702	Add kernel related log messages for protocol attacks.
397714	Need a *fill log disk* utility to assist with CC testing.
398802	Forward traffic log shows `dstintf=unknown-0` after enabling antivirus.
401511	FortiGate Local Report showing incorrect *Malware Victims* and *Malware Sources*.
402712	Username truncated in Webfilter & DLP logs.
406071	DNS filtering shows error: *all Fortiguard SDNS servers failed to respond*.
417128	Syslog message are missed in Fortigate.
421062	FortiGate 60E stopped sending logs to FortiAnalyzer when reliable enabled.

Router

Bug ID	Description
373892	ECMP(BGP) routing failover time.
374306	Number of concurrent sessions affect the convergence time after HA failover.
383013	Message `ha_fib_rtnl_hdl: msg truncated, increase buf size` showing up on console.
385264	AS-override has not been applied in multihop AS path condition.
392250	BGP session not establishing with Cisco Nexus.
393623	Policy routing change not is not reflected.
397087	VRIP cannot be reached on 51E when it is acting as VRRP master.
399415	Local destined IPv6 traffic matched by PBR.
405408	FortiGate creates corrupted OSPF LS Update packet when certain number of networks is propagated.
421151	ICMP redirect received in root affects another VDOM's route gateway selection.

SSL VPN

Bug ID	Description
370986	SSL VPN LDAP user password renew doesn't work when two factor authentication is enabled.
375827	SSL VPN web mode get `Access denied` to FOS 5.4.1 GA B1064 under VDOM.
375894	SSL VPN web mode access FMG B1066/FAZ B1066 error.
387276	SSL VPN should support Windows 10 OS check.
389566	"AltGr" key does not work when connecting to RDP-TLS server through SSL VPN web portal from IE 11.
394272	SSL VPN proxy mode can't proxy some web server URL normally.
395497	`https-redirect` for SSL VPN does not support realms.
396932	Some web sites not working over web SSL VPN.
399711	SSL VPN does not decode `hostcheck` string properly for latest FortiClient.
399784	URL modified incorrectly for a dropdown in application server.
402743	User peer causes SSL VPN access failure even though user group has no user peer.
405799	AV breaks login to OWA via SSL VPN web mode.
406028	Citrix with Xenapp 7.x not working via SSL VPN web portal.
408624	SSL VPN certificate UPN+LDAP authentication works only on first policy.
423452	Citrix Xenapp not working properly via SSL VPN web portal.

System

Bug ID	Description
182287	Implementation for `check_daemon_enable()` is not efficient.
283952	VLAN interface Rx bytes statistics higher than underlying aggregate interface.
302722	Using CLI `#get system hardware status` makes CLI hang.
306041	SSH error `Broken pipe` on client when using remote forwarding and SSH deep packet option `log port fwd` is enabled.

Bug ID	Description
354490	False positive sensor alarms in Event log.
355256	After reassigning a hardware switch to a TP-mode VDOM, bridge table does not learn MAC addresses until after a reboot.
375798	Multihoming SCTP sessions are not correctly offloaded.
376423	Sniffer is not able to capture ICMPv6 packets with *Hop-by-Hop* option when using filter *icmp6*.
377192	DHCP request after lease expires is sent with former unicast IP instead of 0.0.0.0 as source.
378364	L2TP over IPsec tunnel cannot be established in FortiGate VM.
379883	Link-monitor doesn't remove the route when it is in "die" state.
381363	Empty username with Radius 802.1x WSSO authentication.
382657	ICMP Packets bigger than 1418 bytes are dropped when offloading for IPsec tunnel is enabled. Affected models: FG-30D, FG-60D, FG-70D, FG-90D, FG-90D-POE, FG-94D, FG-98D, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FWF-30D, FWF-60D, FWF-90D, FWF-90D-POE.
383126	50E/51E TP mode - STP BPDU forwarding destined to 01:80:c2:00:00:00 has stopped after warm/cold reboot.
385455	Inconsistent trusted host behavior.
385903	Changing `allowedaccess` on FG-200D hardware switch interfaces causes hard-switch to stop functioning.
386271	On FWF-90D after enabling IPS sensor with custom sig, in 60% chance need to wait for 30+ seconds to let ping packet pass.
386395	Missing admin name in system event log related to admin NAC quarantine.
388971	Insufficient guard queue size when sending files to FSA.
389407	High memory usage for `radvd` process.
389711	Suggest asic_pkts/asic_bytes counter in `diagnose firewall iprope show` should remain after FortiGate reboot.
391168	Delayed Gratuitous ARP during SLBC Chassis Fail-back.
391460	FortiGuard *Filtering Services Availability* check is forever loading.

Bug ID	Description
392655	Conserve mode - 4096 SLAB leak suspected.
393275	VDOM admin forced change password while there is other login session gets *The name is a reserved keyword by the system*.
393343	Remove botnet filter option if interface role is set to LAN.
394775	GUI not behaving properly after successful upload of FTK200CD file.
395039	Loopback interface: Debug Flow and logs do not show the usage of firewall policy ID.
396018	Backup slave member of a redundant interface accept and process incoming traffic.
397984	SLBC - FIB sync may fail if there is a large routing table update.
398424	On some models, after upgrading from FortiOS 5.4.1 to 5.4.2 build 1100, crashlog occurs when booting.
398852	UDP jumbo frames arrives fragmented on a 3600C are blocked when acceleration is enabled.
399364	VDOM config restore fails for GRE interface bound to IPsec VPN interface.
399648	LAN ports status is up after reboot even if administrative status is down on FG-30D.
400907	Ethernet Ports Activity LED doesn’t light for shared copper ports.
401360	LDAP group query failed when the fixed length buffer overflows.
402742	VDOM list page does not load.
403532	FG-100D respond fragmented ICMP request with non-fragmented reply right after factory reset.
403724	Real number of FortiToken supported doesn't match tablesize on some platforms.
403937	High memory on VSD.
404258	L2TP second user cannot connect to FG-600D via a router (NAPT).
404480	Link-monitor is not detecting the server once it becomes available.
405234	Unable to load application control replacement message logo and image in explicit proxy (HTTPS).
405757	Interface link not coming up when FortiGate interface is set to *1000full*.

Bug ID	Description
406071	DNS Filtering showing error `all Fortiguard SDNS servers failed to respond`.
406519	Administrative users assigned to *prof_admin* profile do not have access to `diagnose` CLI command.
406689	Autoupdate schedule time is reset after rebooting.
406972	Device become unresponsive for 30 min. during IPS update when `cfg-save` option is set to manual.
409828	Cisco switches don't discover FortiGate using LLDP on internalX ports.
410463	SNMP is not responding when queried on a loopback IP address with an asymmetric SNMP packet path.
410901	PKI peer CA search stops on first match based on CA subject name.
411432	`scanunitd` gets high CPU when making configuration changes.
411433	`voipd` shows high CPU when making configuration changes.
411685	If IPPool is enabled in the firewall policy, offloaded traffic to NP6 is encrypted with a wrong SPI.
414243	DNS Filter local FortiGuard SDNS servers failed to respond due to malformed packet.
416678	FG101E/100E has reports of firewall lockups in production.
418205	High CPU utilization after upgrade from FortiOS 5.2.10 to 5.4.4.
420170	Skip the rating for dynamic DNS update type queries.

Web Filter

Bug ID	Description
188128	For the Flowbase web filter, the CLI command `set https-replacemsg disable` does not work.

WebProxy

Bug ID	Description
376808	Explicit proxy PAC File distribution in FortiOS 5.4.x not working properly.

Bug ID	Description
383817	WAD crashes with a signal 11 (segmentation fault) in `wad_port_fwd_peer_shutdown` and `wad_http_session_task_end`.
389863	Signal 11 WAD and HTTPSD processes, and GUI not accessible.
398052	WAD session leak.
398405	WAD crashes without backtrace.
400454	Improve WAD debug trace and crash log information.
402155	WAS crashes with signal 6 in `wad_authenticated_user_authenticate` after upgrade to 5.4.3.
402778	WAD does not authorize user if it belongs to more than 256 usergroups with Kerberos authentication.
405264	WAD crash when flush FTP over HTTP traffic.
408503	Cannot access websites when *SSL Inspection* is set to *Inspect All Ports* with Proxy Option enabled only for HTTP(ANY).
412462	Fortinet-Bar does not show up on iPhone with iOS 10.2.1 Safari and Google Chrome 57.0.2987.100.
415918	Explicit proxy users are disconnected once a VDOM is created / removed.
421092	WAD consuming memory when explicit webproxy is used.

WiFi

Bug ID	Description
387146	Wireless client RSSO authentication fails after reconnection to AP.

Common Vulnerabilities and Exposures

Bug ID	CVE references
408239	FortiOS5.4.5 is no longer vulnerable to the following CVE Reference: • 2015-8874 • 2016-5766 • 2016-5767 • 2016-6128 • 2016-6132 • 2016-6207 • 2016-6912 • 2016-9317 • 2016-10166 • 2016-10167 • 2016-10168 Visit https://fortiguard.com/psirt for more information.
409913	FortiOS5.4.5 is no longer vulnerable to the following CVE Reference: • 2017-3130 Visit https://fortiguard.com/psirt for more information.
421739	FortiOS5.4.5 is no longer vulnerable to the following CVE Reference: • 2017-7734 • 2017-7735 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.4.5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
374969	FortiSandbox FortiView may not correctly parse the FSA v2.21 tracer file(.json).

DLP

Bug ID	Description
435283	`block-page-status-code` doesn't work for HTTP status code of the DLP replacement message.

Endpoint Control

Bug ID	Description
374855	Third party compliance may not be reported if FortiClient has no AV feature.
375149	FortiGate does not auto update AV signature version while Endpoint Control is enabled.
391537	Buffer size is too small when sending large vulnerability list to FortiGate.

Firewall

Bug ID	Description
364589	LB VIP slow access when cookie persistence is enabled.

FortiGate-3815D

Bug ID	Description
385860	FortiGate-3815D does not support 1GE SFP transceivers.

FortiGate and FortiWifi E Series

Bug ID	Description
413699	In some FortiGate and FortiWifi E series models, the default *Inspection Mode* is flow-based instead of proxy-based. Affected models: FG-60E, FG-61E, FWF-60E, FWF-61E, FG-80E, FG-81E, FG-80E-POE, FG-81E-POE, FG-100E, FG-101E, FG-100EF, FG-140E, FG-140E-POE.

FortiRugged-60D

Bug ID	Description
375246	`invalid hbdev dmz` may be received if the default `hbdev` is used.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully but fails to pass traffic until you reboot FortiSwitch.
374346	Adding or reducing stacking connections may block traffic for 20 seconds.

FortiView

Bug ID	Description
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
372350	*Threat view: Threat Type and Event* information is missing in the last level of the threat view.
372897	`Invalid -4` and `invalid 254` is shown as the submitted file status.
373142	*Threat: Filter* result may not be correct when adding a filter on a threat and threat type on the first level.
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
375187	Using realtime auto update may increase chrome browser memory usage.

GUI

Bug ID	Description
289297	Threat map may not be fully displayed when screen resolution is not big enough.
297832	Administrator with read-write permission for *Firewall Configuration* is not able to read or write firewall policies.
355388	The *Select* window for remote server in remote user group may not work as expected.
365223	CSF: downstream FGT may be shown twice when it uses hardware switch to connect upstream.
365317	Unable to add new AD group in second FSSO local polling agent.
365378	You may not be able to assign `ha-mgmt-interface` IP address in the same subnet as another port from the GUI.
368069	Cannot select `wan-load-balance` or members for incoming interface of IPsec tunnel.
369155	There is no `Archived Data` tab for email attachment in the DLP log detail page.
372908	The interface tooltip keeps loading the VLAN interface when its physical interface is in another VDOM.
372943	Explicit proxy policy may show a blank for default authentication method.
374081	`wan-load-balance interface` may be shown in the address associated interface list.
374162	GUI may show the modem status as `Active` in the `Monitor` page after setting the modem to disable.
374224	The *Ominiselect* widget and *Tooltip* keep loading when clicking a newly created object in the *Firewall Policy* page.
374320	Editing a user from the *Policy* list page may redirect to an empty user edit page.
374322	*Interfaces* page may display the wrong MAC Address for the hardware switch.
374373	*Policy View: Filter* bar may display the IPv4 policy name for the IPv6 policy.
374397	Should only list `any` as destination interface when creating an explicit proxy in the TP VDOM.
374521	Unable to *Revert* revisions in GUI.
374525	When activating the *FortiCloud/Register-FortiGate*, clicking *OK* may not work the first time.

Bug ID	Description
375346	You may not be able to download the application control packet capture from the forward traffic log.
373363	Multicast policy interface may list the `wan-load-balance interface`.
373546	Only 50 security logs may be displayed in the *Log Details* pane when more than 50 are triggered.
374363	Selecting *Connect to CLI* from managed FAP context menu may not connect to FortiAP.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.
375227	You may be able to open the dropdown box and add new profiles even though errors occur when editing a *Firewall Policy* page.
375259	`Addrgrp` editing page receives a `js` error if `addrgrp` contains another group object.
375369	May not be able to change IPsec `manualkey config` in GUI.
375383	Policy list page may receive a `js` error when clicking the search box if the policy includes `wan-load-balance interface`.
379050	User Definition intermittently not showing assigned token.
421423	Cannot download certificate in *Security Profiles* > *SSL/SSH Inspection*. Workaround: Go to *System* > *Certificates* to download.

HA

Bug ID	Description
399115	ID for the new policy (when using edit 0) is different on master and on slave unit.

IPsec

Bug ID	Description
393958	Shellshock attack succeeds when FGT is configured with `server-cert-mode replace` and an attacker uses `rsa_3des_sha`.
408321	If phase2 proposal is configured as `NULL-MD5` encryption, the remote gateway in `diag vpn tunnel list` is changed after receiving traffic from IPsec tunnel.
435124	Cannot establish IPsec phase1 tunnel after upgrading from version 5.4.5 to 5.6.0. Workaround: After upgrading to 5.6.0, reconfigure all IPsec phase1 `psksecret` settings.
439923	IKE static tunnels using `set peertype one` may fail to negotiate.

Router

Bug ID	Description
299490	During and after failover, some multicast groups take up to 480 seconds to recover.

SSL VPN

Bug ID	Description
303661	The Start Tunnel feature may have been removed.
304528	SSL VPN Web Mode PKI user might immediately log back in even after logging out.
374644	SSL VPN tunnel mode Fortinet bar may not be displayed.
375137	SSL VPN bookmarks may be accessible after accessing more than ten bookmarks in web mode.
382223	SMB/CIFS bookmark in SSL VPN portal doesn't work with DFS Microsoft file server error "Invalid HTTP request".

System

Bug ID	Description
284512	When using the Dashboard *Interface History* widget, the httpds process uses excessive memory and then crashes.
287612	Span function of software switch may not work on FortiGate-51E/FortiGate-30E.
290708	`nturbo` may not support CAPWAP traffic.
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
304199	FortiLink traffic is lost in HA mode.
364280	User cannot use `ssh-dss` algorithm to log in to FortiGate via SSH.
371320	`show system interface` may not show the *Port* list in sequential order.
372717	Option `admin-https-banned-cipher` in `sys global` may not work as expected.
392960	FOS support for V4 BIOS.
424215	FG-80C halts during boot after upgrade from 5.2.10 to 5.4.4.

Upgrade

Bug ID	Description
269799	`Sniffer config` may be lost after upgrade.
273973	When upgrading from 5.2 to 5.4, the Central NAT feature cannot be upgraded. After the upgrade, reconfigure the Central NAT feature. Please see the configuration examples in the FortiOS Handbook available in the Fortinet Document Library.
289491	When upgrading from 5.2.x to 5.4.0, port-pair configuration may be lost if the `port-pair` name exceeds 12 characters.

Visibility

Bug ID	Description
374138	FortiGate device with VIP configured may be put under Router/NAT devices because of an address change.

VM

Bug ID	Description
364280	`ssh-dss` may not work on FGT-VM-LENC.

WiFi

Bug ID	Description
434991	WTP tablesize limitation cause WTP entry to be lost after upgrade from v5.4.4 to 5.4.5. Affected models: FG-30D, FG-30D-POE, FG-30E, FWF-30D, FWF-30D-POE, FWF-30E.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

High Performance Network Security